4)

DEPARTMENT OF COMMERCE · UNITED STATES OF AMERICA ·

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

MF

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR		ATTORNEY DOCKET NO.
09/023,672	02/13/98	SCHEIDT	E	STS-119

023995 TM02/0406
RABIN & CHAMPAGNE, PC
1101 14TH STREET, NW
SUITE 500
WASHINGTON DC 20005

EXAMINER	
DARROW, J	
ART UNIT	PAPER NUMBER
2132	17

DATE MAILED: 04/06/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Paper No. 17

Application Number: 09/023,672
Filing Date: February 13, 1998
Appellant(s): Scheidt et al.

Thomas M. Champagne
For Appellant

EXAMINER'S ANSWER

This is in response to appellant's brief on appeal filed February 12, 2001.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying that there are no related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief was correct. Upon review of the appeal brief, the grounds of rejection for claims 3-34, 37-65, and 67-69 are no longer considered applicable. The new status of claims is claims 1, 2, 35, 36, and 66 are appealed and claims 3-34, 37-65, and 67-69 are objected to.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is substantially correct for claims 1, 2, 35, 36, and 66.

The appellant's statement of the issues in the brief is substantially correct. The changes are as follows:

Claims 3-34, 37-65, and 67-69 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

Claims 3 and 37 are drawn to a cryptographic key split combiner and a process of forming cryptographic keys including generating a random sequence based on reference data, respectively. The closest prior art, Hirsch in view of Albert et al., discloses a similar combiner and process. However, they neither teach nor suggest generating a random sequence based on the reference data. This particular limitation explicitly recited in claims 3 and 37 renders them to have allowable subject matter.

Claims 4 and 38 are drawn to a cryptographic key split combiner and a process of forming cryptographic keys including generating a pseudorandom sequence based on reference data, respectively. The closest prior art, Hirsch, delineates a similar combiner and process. However, he neither describes nor implies generating a pseudorandom sequence based on the reference data. This distinct feature explicitly recited in claims 4 and 38 renders them to have allowable subject matter.

Claims 5 and 39 are drawn to a cryptographic key split combiner and a process of forming cryptographic keys including generating a random sequence based on reference data and on chronological data, respectively. The closest prior art, Hirsch in view of Thomlinson et al., elaborates on a similar combiner and process. However, they neither disclose nor suggest generating a random sequence based on the reference data and on chronological data. This limitation explicitly written into claims 5 and 39 renders them to have allowable subject matter.

Claims 6-8 and 40-42 are drawn to a cryptographic key split combiner and a process of forming cryptographic keys including generating a random sequence based on reference data and on static data, respectively. The closest prior art, Hirsch in view of Ming et al., discloses a similar combiner and process. However, they neither mention nor imply generating a random sequence based on the reference data and on static data. This distinct feature explicitly recited in claims 6 and 40 renders them and dependent claims 7 and 8; and 41 and 42, respectively, to have allowable subject matter.

Claims 9-17 and 43-51 are drawn to a cryptographic key split combiner and a process of forming cryptographic keys including generating a token key split based on label data, respectively. The closest prior art, Hirsch in view of Ming et al., describes a similar combiner and process. However, they neither discuss nor suggest generating a token key split based on label data. This particular limitation explicitly included in claims 9 and 43 renders them and dependent claims 8-17 and 44-51, respectively, to have allowable subject matter.

Claims 18-24 and 52-58 are drawn to a cryptographic key split combiner and a process of forming cryptographic keys including generating a console key split based on maintenance data, respectively. The closest prior art, Hirsch in view of Anshel et al., delineates a similar combiner and process. However, they neither disclose nor imply generating a console key split based on maintenance data. This distinct feature explicitly recited in claims 18 and 52 renders them and dependent claims 19-24 and 53-58, respectively, to have allowable subject matter.

Claims 25-31 and 59-65 are drawn to a cryptographic key split combiner and a process of forming cryptographic keys including generating a biometric key split based on biometric data, respectively. The closest prior art, Hirsch in view of Tomko et al., teaches a similar combiner and process. However, they neither elaborate on nor suggest generating a console key split based on maintenance data. This distinct feature explicitly recited in claims 25 and 59 renders them and dependent claims 26-31 and 59-65, respectively, to have allowable subject matter.

Claims 32 and 67 are drawn to a cryptographic key split combiner for forming cryptographic keys and a cryptographic key which is a stream of symbols, respectively. The closest prior art, Hirsch, delineates a similar combiner and key. However, he neither teaches nor implies steam of symbols. This distinct feature explicitly recited in claims 32 and 67 renders them to have allowable subject matter.

Claims 33 and 68 are drawn to a cryptographic key split combiner for forming cryptographic keys and a cryptographic key which is at least one symbol block, respectively. The closest prior art, Hirsch, describes a similar combiner and key. However, he neither shows nor suggests at least one symbol block. This particular limitation explicitly written in claims 33 and 68 renders them to have allowable subject matter.

Claims 34 and 69 are drawn to a cryptographic key split combiner for forming cryptographic keys and a cryptographic key which is a key matrix, respectively. The closest prior art, Hirsch, describes a similar combiner and key. However, he neither shows nor suggests a key matrix. This distinct feature explicitly recited in claims 34 and 69 renders them to have allowable subject matter.

(7) Grouping of Claims

The appellant's statement in the brief that certain claims do not stand or fall together is not agreed with because the appellants arguments concerning the appealed claims in Group 1, claims 1, 2, 35, 36, and 66, are directed only to the limitations explicitly recited in claim 1. Although claim 66 is not listed in the appellant's statement, it is not separately patentable from claims 1, 2, 35, and 36.

Although the appellant's brief includes a statement that claims 1, 2, 35, 36, and 66 do not stand or fall together, he provides no reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

4,145,568	EHRAT	3-1979	*
4,864,616	POND	9-1989	*
5,276,738	HIRSCH	1-1994	
5,541,994	TOMKO	7-1996	
5,627,894	ALBERT	5-1997	
5,710,815	MING	1-1998	
5,751,808	ANSHEL	5-1998	
5,778,069	THOMLINSON	7-1998	

R/ * Newly cited references. ☒ Pertinent to disclosure but not relied upon.

(10) Grounds of Rejection

The following grounds of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1, 2, 35, 36, and 66 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Hirsch, U.S. Patent No. 5,276,738.

As per claims 1, 35, and 66, Hirsch illustrates a cryptographic key split combiner, a process for combining, and a key formed by the process comprising: a plurality of key split generators for generating cryptographic key splits (see column 1, lines 57-67); and a key split randomizer for randomizing the cryptographic key splits to produce a cryptographic key (see column 1, lines 54-57 and lines 62-68; column 2, lines 1-7; column 3, lines 60-65; and figure 1A, items 10, 12, and 16); in which each of the key split generators includes means for generating key splits from seed data (see column 1, lines 49-54 and lines 62-64).

As per claims 2 and 36, Hirsch further teaches that the plurality of key split generators includes a random split generator for generating a random key split based on reference data (see column 2, lines 55-58).

(11) Response to Argument

As per claims 1, 2, 35, 36, and 66, Hirsch clearly states a cryptographic key split combiner comprising: a plurality of key split generators (see "multibit container location" in column 1, lines 57-58) for generating cryptographic key splits (see "unique sequence of random number values" in column 1, lines 58-59); and a key split randomizer for randomizing the cryptographic key splits to produce a cryptographic key (see "scrambler" in column 1, lines 54-55); in which each of the key splits generators includes means for generating key splits from seed data (see "stored input binary value" in column 1, line 62). Thus, in this disclosure the key splits are the individual bits of the "stored input binary number rearrang[ed] . . . as a function of the random number values," (see column 1, lines 62-64) and the their respective complements (see column 3, lines 65-68); the seed data of which the key splits are generated are the individual bits of the stored input binary number (see column 1, lines 62-64) and the "different one[s] of a unique sequence of random number values (see column 1, lines 57-59); and the key split randomizer for randomizing the key splits to produce a cryptographic key is "exclusive or means for performing an exclusive or of the numeric value of bit position of the input binary bit applied as an input . . . with the random number stored in the container . . . [in which] the least significant bit of the result . . . defines if the input binary bit or its complement is to be applied as an output of the container" (see column 3, lines 60-68 and column 4, lines 1-10). The appellant's assertion that Hirsch discloses "a plurality of containers in a single scrambler array which together receive a single 32-bit value that is modified according to a serially-shifted pseudorandom sequence generated from a single seed" (see Appeal Brief, page 10, line 23 and page 11, lines 1-2) is not correct. The containers represent key split generators which contain key splits (see column 1, lines 57-59) generated from different seeds (see column 2, lines 19-34). The appellant's assertion that Hirsch "taking a single 32-bit modified value, and mapping 8-bit segments of that value according to a stored, predetermined, fixed table, to generate a key" (see Appeal Brief, page 11, lines 5-7) is also not correct. There is no predetermined table disclosed. Table 204 represented in column 4, lines 50-68 and column 5, lines 1-13 is the result of the randomization depicted in figure 1C for the specific embodiment that Hirsch discloses.

(12) Conclusion

The appellants have not distinguished the invention of claims 1-5, 7-11, and 19-27 over the prior art of record. Therefore, for the above reasons, the rejections should be sustained.

Respectfully submitted,

JD

JTD

Examiner

GB

GILBERTO BARRON, JR.
PRIMARY EXAMINER
ART UNIT ~~222~~ 2132
conferee

Gilberto Barron, Jr.

Appeal Conferee

April 3, 2001

TOD SWANN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Thomas M. Champagne
RABIN & CHAMPAGNE, P.C.
1101 14th Street, N.W.
Suite 500
Washington, DC 20005